Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently Amended) A method for the secure distribution of digitised audio-visual works ("media") to consumers over a data network comprising the steps of:

encrypting said media using a different encryption key for each work ("media key"),

storing the encrypted media on one or more first servers,

storing the media keys on a second server,

making available one or more retail servers from which consumers may obtain the right to receive media keys for desired media in exchange for complying with conditions set by the retailer,

creating steering files corresponding to each media work and its corresponding key, said steering files containing information identifying the media work and the location of the media key and the location of the corresponding media work,

making available said steering files on said one or more retail servers,

the consumer causing a request to be made from a network-connected client device to a selected retail server for at least the media key for a desired media work,

said steering files when processed on said client device causing a request to be made to said second server for the key for the media work identified in the steering file and causing the client device to generate said request to the first server identified in said steering file to supply the encrypted media work,

at the selected retail server, verifying the consumer has complied with the retailer's conditions, and if so,

the retail server either passing said request to the second server, or supplying to the client device data allowing the second server to be contacted,

at said second server verifying the allowability of fulfilling requests from said retail server or a client device and if so allowable encrypting the relevant media key and downloading it to either said retail server or said client device,

said retail server if receiving an encrypted media key from said second server, downloading said encrypted media key to said client device,

at the client device decrypting the received media key and storing it in memory in either encrypted or decrypted form,

subsequently, at the client device generating a request to the appropriate first server to supply the desired media work,

from the first server downloading the desired encrypted media work downloading the encrypted media work to said client device, and

at the client device retrieving the media key from said memory and using it to decrypt the media work to a condition where it can be played using appropriate player software.

2. (Original) A method according to claim 1 wherein at the client device the encrypted media key is stored in memory in encrypted form and when the encrypted media work is downloaded to said client device the encrypted media key is retrieved from memory, decrypted and used to decrypt the media work.

3. Cancelled

4. Cancelled

5. (Original) A method according to either of claims 1 or 2 wherein said second server encrypts media keys for consumers using a public key encryption algorithm and when said client device generates a request to either said retail server or said second server for a media key it includes in the request the consumer's public key, said second server encrypting the relevant media key with the consumer's public key and upon receipt of said encrypted media key said client device decrypting the key using the consumer's private key.

6. (Original) A method as claimed in either of claims 1 or 2 wherein the client device stores the media key in volatile memory.

7. (Original) A method according to either of claims 1 or 2 wherein said retail server passes received client device requests to said second server and said second server upon verifying the allowability of fulfilling requests from said retail server downloading the encrypted media key to said retail server.

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)